EDUZONE: International Peer Reviewed/Refereed Multidisciplinary Journal (EIPRMJ), ISSN: 2319-5045
Volume 13, Issue 1, January-June, 2024, Available online at: www.eduzonejournal.com

Face Spoof Detection Techniques: A Survey

Ramandeep Kaur[1], Er. Sonia Digra[2]

[1]M. Tech (ECE) Research Scholar), Golden Group of Engineering and Technology, Gurdaspur
[2]HOD ECE, Golden Group of Engineering and Technology, Gurdaspur

ABSTRACT

The face spoof detection is frequently used with various microscopic biometric modalities. Based on artificial intelligence, The face spoof detection techniques have various phases which include pre-processing, feature extraction and classification. In this paper, the different types of methods used in face spoof detection have been discussed. Various types of feature extraction algorithms are used which can be categorized as textural feature and colour feature extraction algorithms. The different schemes for the face spoof detection have been reviewed which are based on machine learning, deep learning and other general techniques. The schemes have been reviewed on basis of methodology and outcomes

Keywords: Face Spoof, Machine Learning, Deep Learning, Face Detection

INTRODUCTION

Applications that require authentication can benefit from the strong and useful solution provided by biometrics. Nowadays, academia and industry are paying more and more attention to biometrics authentication thanks to deep learning because of its advancements in security compared to more conventional authentication techniques (such passwords, secret questions, and token codes) [1]. The most common biometric modalities are voice, iris, face, and fingerprints. Of them, "face" is the most widely used because it doesn't require any extra hardware resource and almost all smartphones come with a front-facing camera. Despite the effectiveness of face recognition, it is still susceptible to presentation attacks because of the prevalence of social media, where it is simple to obtain facial photos.As an illustration, a presentation assault can capture a person's facial information by printing (printing attack), replaying on a screen (replay attack), or even forging the face using 3D masking and VR, which poses highly difficult security challenges [2]. Numerous studies for face spoofing detection have been prompted by security issues with face recognition systems. A number of methods attempt to recover the distortion information that may be present in spoof face samples from the perspective of evaluating the disturbance information put into the spoofing media. Common spoofing artefacts include those related to texture, motion, and image quality. The facial recognition system may be tricked by imitating genuine faces.Before detecting facial photos, anti-spoofing technologies must be put in place to thwart these attacks. The security of the facial recognition system must be ensured [3].

If spoof attack attempts are made on an ordinary face recognition system that lacks intentional and concrete anti-spoofing features (as is the case with many face recognition systems in use), the system is likely to fail. Respondents provide the face recognition system with their facial features, which it then compares to the information in the base library ID. The system will regard the respondent as "real" and grant access to the main system if the comparison result score is less than the threshold. Even while the facial recognition technology has made great progress, it occasionally still confuses real faces with fraudulent ones [4]. A generalised depiction of a face recognition system is shown in Fig. 1.

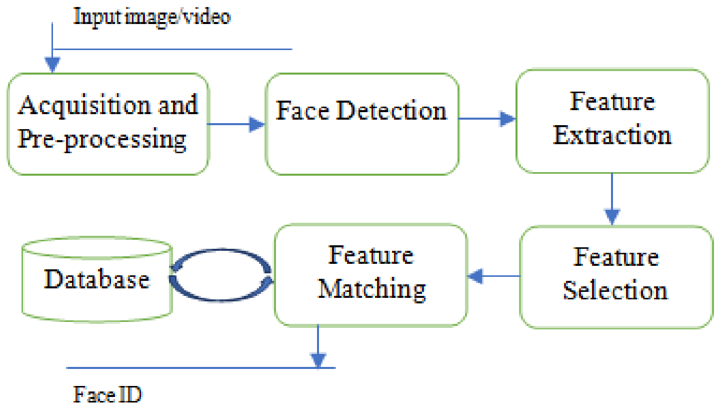

Figure 1: Pipeline of a Face Recognition System

Image capture and pre-processing are the first stages taken by every picture processing system for features extraction and image understanding. The input source, which can be either static images or streaming video, is used to generate the target images. Image processing systems must include picture pre-processing in order to achieve accurate results while also minimizing noise [5]. Systems in this condition must confront a wide range of challenges that could obstruct the entire process, especially in an unconstrained environment. These issues could include, among other things, variations in the image background, attitude, ageing, illumination, and expressions. Given that it has an impact on how well feature extraction functions, pre-processing a picture is always recommended as one of the first processes [6].Post-processing of data might be considered for the removal of noise from the given image in the case of an uncontrolled environment where learning is influenced by external variables. Facial detection is the process of locating and isolating the face region from the surrounding area. It is a further critical step in the overall facial recognition process and has undergone substantial research in the field of machine vision. Early face recognition techniques were able to swiftly recognise facial features in input photographs [7]. It eventually became a vibrant study area and a fundamental part of any framework for understanding faces visually.

The first task of any face recognition system is feature extraction. It has a significant impact on the system's overall effectiveness. There are different varieties of feature extractor models, such as SIFT, SVM, STIP, and STISM. A variety of criteria have been used to categorise feature extraction techniques, including global vs. local [8], hand-crafted vs. learning-driven, and 2D vs. 3D features extraction schemes. Feature extractors or descriptors commonly generate a large feature space for a single image when attempting to identify a person in a streaming video. The huge feature space is then further processed using a variety of techniques in order to narrow down the most crucial features and lessen dimensionality.This enhances system performance by lowering total expenses and making better use of the system period for recognition [9]. The primary features are taken from the input facial image and then iteratively matched to meet the goal objective. Face recognition that is iterative is a process. The identifier is just taken out of the database by the system. Researchers have proposed a substantial number of remedies in the research as a result of the recent increase in interest in face spoof detection. Three different face spoofing detection techniques are briefly discussed in this section: texture-based techniques, motion-based techniques, and picture quality and reflectance-based techniques[10]. Since the bulk of face recognition systems only employ RGB cameras, integrating texture information has been an obvious approach for preventing face spoofing.Numerous texture-based features are researched in this domain to prevent face faking. CNN-based features and handcrafted features can be readily divided from two categories. ConvNet-conditioned features or ConvNets have been used in face anti-spoofing in multiple recent attempts as a result of deep learning's success in resolving a wide range of computer vision issues. The majority of research techniques approach anti-spoofing as a straightforward binary classification issue with softmax loss. To defend against display and picture attacks, motion-based approaches use facial movements such moving lips, blinking eyes, and other facial expressions [11]. By replicating the varying stages of eye blinking, eye movement is used as an effective cue for face anti-spoofing.The detection of spoofing attacks also makes use of mouth movement in tandem with eye blinking. The approaches based on image quality and reflectance are reviewed in the literature since the recovered picture and video may result in a loss of image quality and variations in reflectance. These methods extract specular reflection, blurriness, chromatic moment, and colour variety from the liquid crystal display (LCD) screen to explain the changes in surface reflection between the real and fake faces [12]. Numerous researchesuse optical flow features and image-quality features to distinguish real faces from fake faces. Furthermore, the elements that are most useful for spotting face spoofing can be extracted by analysing the noise information in phoney face photographs using the Fourier spectrum [13].These reflectance- and image-based approaches defend against low-resolution attacks well, but they may fall short when faced with spoof artefacts that are incredibly convincing.

LITERATURE REVIEW

W. Zhang, et.al (2020) suggested a FAS (face anti-spoofing) technique in which DWT, LBP and DCT (Discrete Cosine Transform) algorithm were implemented with a SVM (Support Vector Machine) for computing the authenticity of a video [14]. First of all,some selected frames were decomposed into diverse frequency elements at the multi-resolution blocks to create attributes of DWT (Discrete Wavelet Transform). After that,LBP (Local Binary Pattern)histograms contained in DWT blocks were related to every frame in horizontal way for producing DWT-LBP features. Hence, the spatial information was presented.In the end, the face spoofing was detected after training SVM algorithm with RBG kernel. REPLAY-ATTACK and CASIA-FASD datasets executed to conduct the experiments. The experimental outcomes validated the efficiency and generalized potential of the suggested technique.

W. Liu, et.al (2022) projected a MDTSC (multimodility data-based two-stage cascade)model to perform face anti-spoofing [15]. Initially, a TSC framework was constructed for fusing the attributes of lower and higher level from diverse modalities so that the feature representation was enhanced. Subsequently, adistance-free spectral was built on RGB and infrared on the basis of multimodality data for augmenting the nonlinearity of data. Furthermore, an MPWF (multiscale patch-based weighted fine-tuning) algorithm was put forward for learning every local face area. The outcomes of experiments demonstrated the supremacy of the projected model over the traditional methods.

H. Chen, et.al (2019) developedFARCNN (face anti-spoofing region-based convolutional neural network) algorithm on the basis of improved Faster R-CNN (region-based convolutional neural network) [16]. This algorithm assisted in classifying the data as real face, forged and background. Various techniques such as RPFF (roi-pooling feature fusion) were optimized and CLF (Crystal Loss function) was inserted to enhance the traditional algorithm. Furthermore, diverse illumination situations were handled using an enhanced Retinex based LBP (Local Binary Pattern)for detecting the face spoofing. The last task was to cascade these two detectors and to attain efficiency on3 datasets namely CASIA-FASD, REPLAY-ATTACK and OULU-NPU. The outcomes reported that the developed algorithm was efficient for detecting face spoofing.

S. Jia, et.al (2021)presented a novel database recognized as SWFFD (Single Wax Figure Face Database)in 4-000 single wax figure faces were comprised [17]. The online resources considered to gather this dataset and it offered higher diversity concerning subjects, lighting conditions, facial poses, and recording devices. Moreover, a novel technique was constructed in which attention-aware attributes were incorporated from diverse face scales for creating discriminative illustrations. Hence, the real face spoofing attack was detected. The experimental results on SWFFD andCelebA-HQ database indicated that the constructed technique was applicable on intra-and cross-database testing scenarios.

G. D. Simanjuntak, et.al (2019) introduced a CDA (color distortion analysis) based approach in order to detect the face spoofing and to capture the chromatic aberration from a face image [18]. This approach emphasized on extracting color moment and ranked histogram attributes for generating 116-feature vector. PCA (Principal Component Analysis) algorithm made the deployment of this approach to mitigate the dimensionality.The image was classified as authentic and spoofed face using NB (Naïve Bayes) algorithm on the basis of PCs (principal components). The experimental results reported that the introduced approach provided a TPR (True Positive Rate) of 97.4% in contrast to other methods.

L. Li, et.al (2018) investigated a new E2E (end-to-end) learnable (Local Binary Pattern)algorithm in order to detect the face spoofing [19]. This algorithm was useful foralleviating the number of network metrics. For this,LC (learnable convolutional) layers were integrated with fixed-parameter LBP layers in whichSBFs (sparse binary filters) and DSGFs (derivable simulated gate functions) were involved.Relay-Attack and CASIA-FA datasets applied in quantifying the investigated algorithm. The experimental results proved the stability of the investigated algorithm on these datasets.
S. Jia, et.al (2021) recommended a new anti-spoofing technique to detect the face spoofing [20]. This technique was planned in accordance with MC_FBC (factorized bilinear coding of multiple color channel) targets at learning subtle differences amid realistic and forged images.The discriminative and fusinginformation was extracted from RGB and YCbCr spaces to formulate a principled solution for detecting 3D (three-dimensional) face spoofing. The recommended technique was computed on WFFD (wax figure face database) consisted of images and videos assuper realistic attacks. The experimental results confirmed that the recommended technique performed more effectively underdissimilar intra-and inter-database testing scenarios.

U. Muhammad, et.al (2022) suggested an ASGS (adaptive spatiotemporal global sampling) method for compensating the camera motion and using the resulting estimation with the objective of encoding the presence and dynamics of the video sequences into a RGB image [21]. For this, the video was divided into slight segments and their GM (global motion)was captured in every segment. The dense sampling was performed, FREAK attributes were extracted and matched, similarity was transformed and aggregation function was exploited to estimate the presented GM. Hence, the Deep Models whose pre-training was done on images, utilized for detecting the PAD attack based on video. The experiments results acquired on 4 standard databases reported that the suggested method was robust and gave insights for further study on detecting spoofed face.

Y. Zhang, et.al (2018) presented an innovative feature called SBP-TOP for dealing with the issue related to detect the face spoofing video [22]. The first task was executed for representing the facial attributes in a more noise-resistant version. The second task aimed to combine the visual attributes having time dimension with its original version.CASIA and MSU MFSD datasets executed to compute the presented approach. The experimental outcomes depicted the effectiveness of the presented feature as compared to the existing methods. Moreover, the accuracy of this approach was calculated 95% on both the datasets. The presented approach led to enhance the efficacy up to 10% on initial dataset and 3.2% on the latter one for detecting the spoofed face.

X. Zhu, et.al (2021) discussed that the major intend was to develop a general classification algorithm fordetecting the face images with SMCs (spoofing medium contours) for simplicity [23]. Therefore, the major concentrate was to accomplish the face anti-spoofing as detecting SMCs from the image. Furthermore, a CEM-RCNN (Contour Enhanced Mask-RegionBased Convolutional Neural Network) algorithm was introduced and trained to detect the spoofed face. This algorithm helped in detecting the existence of the SMCs. For this, the contour objectness was included for computing the capacity of an object for containing SMCs. The experimental outcomes revealed that the introduced algorithm was robust to recognize the face images withSpoofing Medium Contours and offered higher accuracy in comparison with the traditional methods.

S. Fatemifar, et.al (2020) developed a stacking ensemble approach to combine an ensemble of one-class classifiers to reduce generalization error in the more plausible undetected attacks [24]. Anomaly samples were not taken into account while designing the Stacking ensemble or when training the constituent anomaly classifiers in order to comply with this situation. This work used client-specific data to develop constituent classifiers and the Stacking combiner in order to improve face-anti spoofing outcomes. In addition, a newer 2-stage genetic algorithm was suggested to further enhance stacking ensemble's generalization performance. Replay-Attack, Replay-Mobile, and Rose-YouTu were three publicly accessible face anti-spoofing databases that were used to assess the effectiveness of the proposed solutions. The benefits of the suggested paradigm were validated by the empirical results that followed the undetected attack evaluation technique.

Table 1: Comparison Table

Author	Year	Technique Used	Results	Limitations
W. Zhang, et.al	2020	FAS (face anti-spoofing) technique	The experimental outcomes validated the efficiency and generalized potential of the suggested technique.	The experiments were not performed in efficient manner as the samples were restricted in amount.
W. Liu, et.al	2022	MDTSC (multimodility data-based two-stage cascade)model	The outcomes of experiments demonstrated the supremacy of the projected model over the traditional methods.	This technique was not able to detect biometric modality attack.
H. Chen, et.al	2019	FARCNN (face anti-spoofing region-based convolutional neural network)	The outcomes reported that the developed algorithm was efficient for detecting face spoofing.	It was not applicable for dealing with all kinds of attacks.
S. Jia, et.al	2021	a novel technique	The experimental results on SWFFD andCelebA-HQ database indicated that the constructed technique was applicable on intra- and cross-database testing scenarios.	This technique attained an ERR of 20% and distinguishing the Super-realistic wax figure faces was difficult.
G. D. Simanjuntak, et.al	2019	CDA (color distortion analysis) based approach	The experimental results reported that the introduced approach provided a TPR (True Positive Rate) of 97.4% in contrast to other methods.	This approach was unable of capturing more generalized attributes.
L. Li, et.al	2018	a new E2E (end-to-end) learnable (Local Binary Pattern)algorithm	The experimental results proved the stability of the investigated algorithm on these datasets.	This algorithm had nor generated optimal results fordetecting some assaults.
S. Jia, et.al	2021	a new anti-spoofing technique	The experimental results confirmed that the recommended	This technique attained an error rate of 10% in many

			technique performed more effectively underdissimilar intra- and inter-database testing scenarios.	scenarios.
U. Muhammad, et.al	2022	ASGS (adaptive spatiotemporal global sampling) method	The experiments results acquired on 4 standard databases reported that the suggested method was robust and gave insights for further study on detecting spoofed face.	This method was not adaptable in real-time and on the biometric systems based on single facial images
Y. Zhang, et.al	2018	SBP-TOP approach	Moreover, the accuracy of this approach was calculated 95% on both the datasets. The presented approach led to enhance the efficacy up to 10% on initial dataset and 3.2% on the latter one for detecting the spoofed face.	This technique was not robust for 3D skin-like real face spoofing assault.
X. Zhu, et.al	2021	CEM-RCNN (Contour Enhanced Mask-RegionBased Convolutional Neural Network) algorithm	The experimental outcomes revealed that the introduced algorithm was robust to recognize the face images withSpoofing Medium Contours and offered higher accuracy in comparison with the traditional methods.	This approach had not detected the SMCs (spoofing medium contours) of some PAs (presentation attacks).
S. Fatemifar, et.al	2020	stacking ensemble approach	The benefits of the suggested paradigm were validated by the empirical results that followed the undetected attack evaluation technique.	This approach consumed much time in some cases.

CONCLUSION

In this paper, it is concluded that various type of techniques is already been proposed for the face spoof detection which can be generally categorized as machine learning, deep learning and general techniques. The feature extraction algorithms are generally being categorized as color feature extraction and textural feature extraction algorithms. It is analyzed that models which are proposed till now for the face spoof detection does not achieve much high accuracy. In future model hybrid model needs to propose for the face spoof detection which achieve high accuracy and also it should be reliable.

REFERENCES

[1]. R. Raghavendra, Kiran B. Raja, Christoph Busch, “Presentation Attack Detection for Face Recognition Using Light Field Camera”, 2015, IEEE Transactions on Image Processing, Vol. 24, No. 3, PP. 1060 - 1075

[2]. Xiao Song, Xu Zhao, Tianwei Lin, “Face spoofing detection by fusing binocular depth and spatial pyramid coding micro-texture features”, 2017, IEEE International Conference on Image Processing (ICIP), Vol. 55, No. 13, PP. 4648-4654

[3]. Hoai Phuong Nguyen, FlorentRetraint, FrédéricMorain-Nicolier, AgnèsDelahaies, "Face spoofing attack detection based on the behavior of noises", 2016, IEEE Global Conference on Signal and Information Processing (GlobalSIP), Vol. 32, No. 9, PP.7582-7589

[4]. HeniEndahUtami, HertogNugroho, "Face Spoof Detection by Motion Analysis on the Whole Video Frames", 2017, 5th International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME), Vol. 21, No. 7, PP. 8993-9001

[5]. L-B. Zhang, F. Peng and M. Long, "Face spoofing detection based on color texture Markov feature and support vector machine recursive feature elimination", Journal of Visual Communication and Image Representation, vol. 49, no. 5, pp. 411-420, February 2018

[6]. M. Yadav and K. Gupta, "Novel Technique for Face Spoof Detection in Image Processing," 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), 2018, pp. 1989-1992

[7]. F. Zhou et al., "Face Anti-Spoofing Based on Multi-layer Domain Adaptation," 2019 IEEE International Conference on Multimedia & Expo Workshops (ICMEW), 2019, pp. 192-197

[8]. L. Li, Z. Xia and H. Han, "Face presentation attack detection based on optical flow and texture analysis", Journal of King Saud University - Computer and Information Sciences, vol. 14, no. 4, pp. 681-691, 5 March 2022

[9]. R. B. Hadiprakoso, H. Setiawan and Girinoto, "Face Anti-Spoofing Using CNN Classifier & Face liveness Detection," 2020 3rd International Conference on Information and Communications Technology (ICOIACT), 2020, pp. 143-147

[10]. L. Lv et al., "Combining Dynamic Image and Prediction Ensemble for Cross-Domain Face Anti-Spoofing," ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2021, pp. 2550-2554

[11]. H. Li, P. He, S. Wang, A. Rocha, X. Jiang and A. C. Kot, "Learning Generalized Deep Feature Representation for Face Anti-Spoofing," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 10, pp. 2639-2652, Oct. 2018, doi: 10.1109/TIFS.2018.2825949.

[12]. G. Heusch, A. George, D. Geissbühler, Z. Mostaani and S. Marcel, "Deep Models and Shortwave Infrared Information to Detect Face Presentation Attacks," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 2, no. 4, pp. 399-409, Oct. 2020

[13]. O. Grinchuk, A. Parkin and E. Glazistova, "3D mask presentation attack detection via high resolution face parts," 2021 IEEE/CVF International Conference on Computer Vision Workshops (ICCVW), 2021, pp. 846-853

[14]. W. Zhang and S. Xiang, "Face anti-spoofing detection based on DWT-LBP-DCT features", Signal Processing: Image Communication, vol. 7, no. 4, pp. 458-464, 2 September 2020

[15]. W. Liu, X. Wei, T. Lei, X. Wang, H. Meng and A. K. Nandi, "Data-Fusion-Based Two-Stage Cascade Framework for Multimodality Face Anti-Spoofing," in IEEE Transactions on Cognitive and Developmental Systems, vol. 14, no. 2, pp. 672-683, June 2022

[16]. H. Chen, Y. Chen, X. Tian and R. Jiang, "A Cascade Face Spoofing Detector Based on Face Anti-Spoofing R-CNN and Improved Retinex LBP," in IEEE Access, vol. 7, pp. 170116-170133, 2019

[17]. S. Jia, C. Hu and Z. Xu, "Face spoofing detection under super-realistic 3D wax face attacks", Pattern Recognition Letters, 3 February 2021

[18]. G. D. Simanjuntak, K. NurRamadhani and A. Arifianto, "Face Spoofing Detection using Color Distortion Features and Principal Component Analysis," 2019 7th International Conference on Information and Communication Technology (ICoICT), 2019, pp. 1-5

[19]. L. Li, X. Feng and A. Hadid, "Face spoofing detection with local binary pattern network", Journal of Visual Communication and Image Representation, vol. 54, no. 1, pp. 182-192, July 2018

[20]. S. Jia, X. Li, C. Hu, G. Guo and Z. Xu, "3D Face Anti-Spoofing With Factorized Bilinear Coding," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 31, no. 10, pp. 4031-4045, Oct. 2021

[21]. U. Muhammad, J. Zhang, L. Liu and M. Oussalah, "An Adaptive Spatio-temporal Global Sampling for Presentation Attack Detection," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 4, no. 6, pp. 721-729, 2022

[22]. Y. Zhang, R. K. Dubey, G. Hua and V. L. L. Thing, "Face Spoofing Video Detection Using Spatio-Temporal Statistical Binary Pattern," TENCON 2018 - 2018 IEEE Region 10 Conference, 2018, pp. 0309-0314

[23]. X. Zhu, S. Li, X. Zhang, H. Li and A. C. Kot, "Detection of Spoofing Medium Contours for Face Anti-Spoofing," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 31, no. 5, pp. 2039-2045, May 2021

[24]. S. Fatemifar, M. Awais, A. Akbari and J. Kittler, "A Stacking Ensemble for Anomaly Based Client-Specific Face Spoofing Detection," 2020 IEEE International Conference on Image Processing (ICIP), 2020, pp. 1371-1375